PHIN Systems Security and Two Factor Authentication

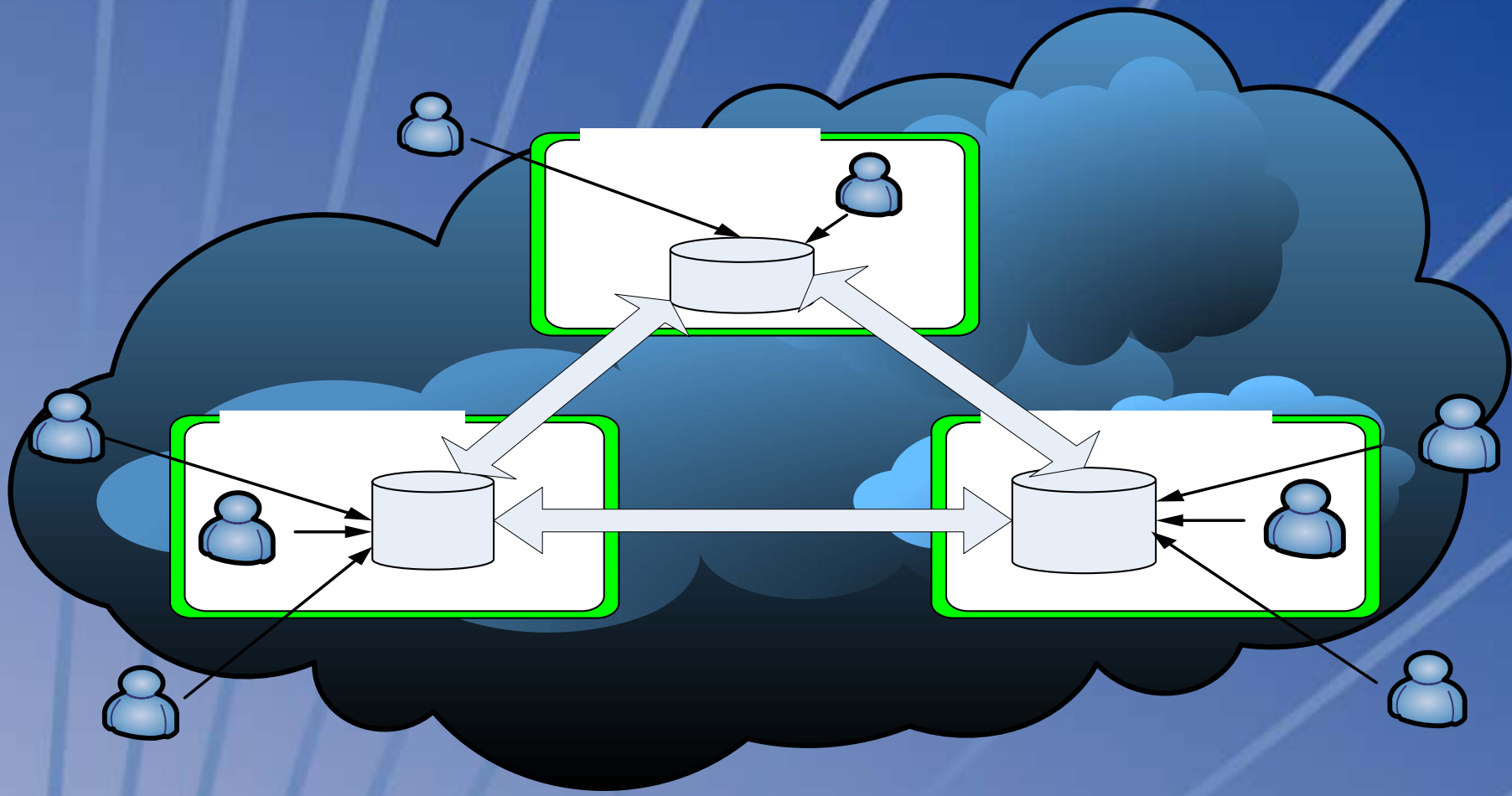
Raja Kailar, Ph.D.
Senior Security Consultant, IRMO/CDC
rok9@cdc.gov, kailar@bnetal.com

SAFER • HEALTHIER • PEOPLE™

Problem Description

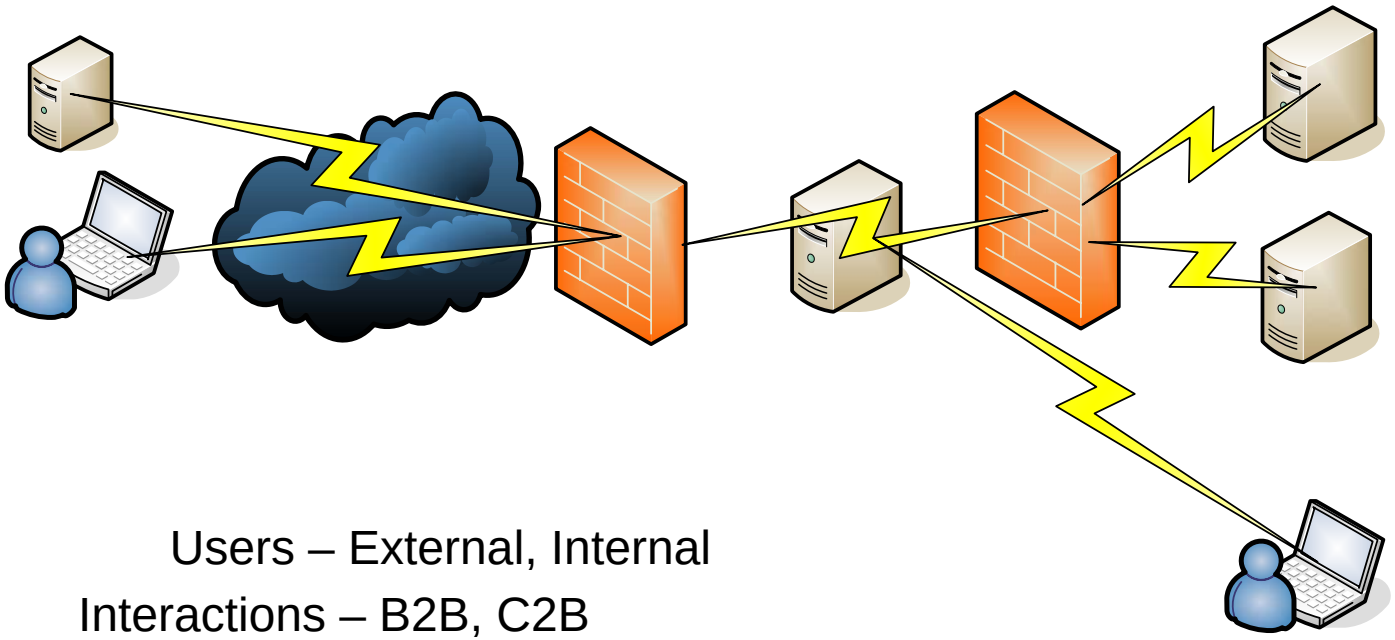
- PHIN – Collaborating partners, sharing public health information over un-trusted networks
- Security depends on reliable identification and authentication (I&A)
- Many public health partners rely solely on login + password for I&A
- Need additional authentication factors for security…

PHIN - Operational Environment



SAFER • HEALTHIER • PEOPLE™

PHIN Users, Interactions, Security Perimeters



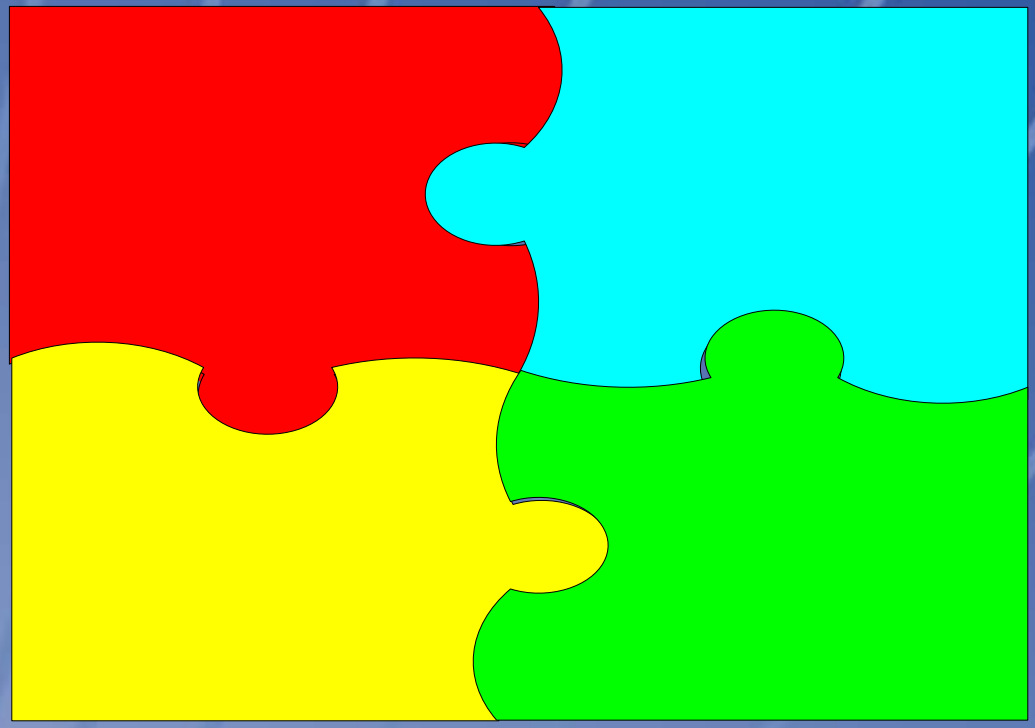
Users – External, Internal

Interactions – B2B, C2B

Perimeter – Firewalls, DMZ

External Application (e.g., Messaging)

High Level Security Requirements

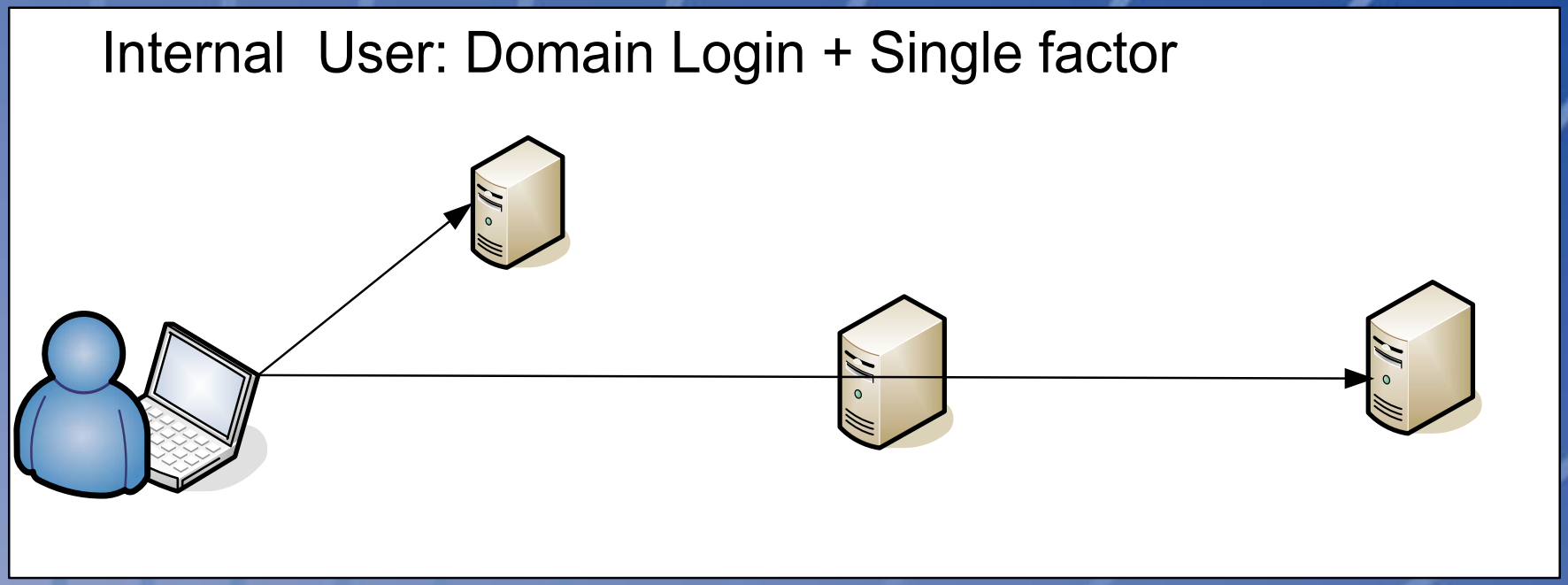


Strong Authentication Important
for most requirements

Authentication Considerations

- What are your PHIN applications? Who are your users?
- Is your user population relatively stationary or mobile?
- From where do your users need to access PHIN applications?
  - Intranet?
  - Internet?
  - Both?
- Does your network infrastructure provide adequate protection to PHIN data (GAP analysis)?

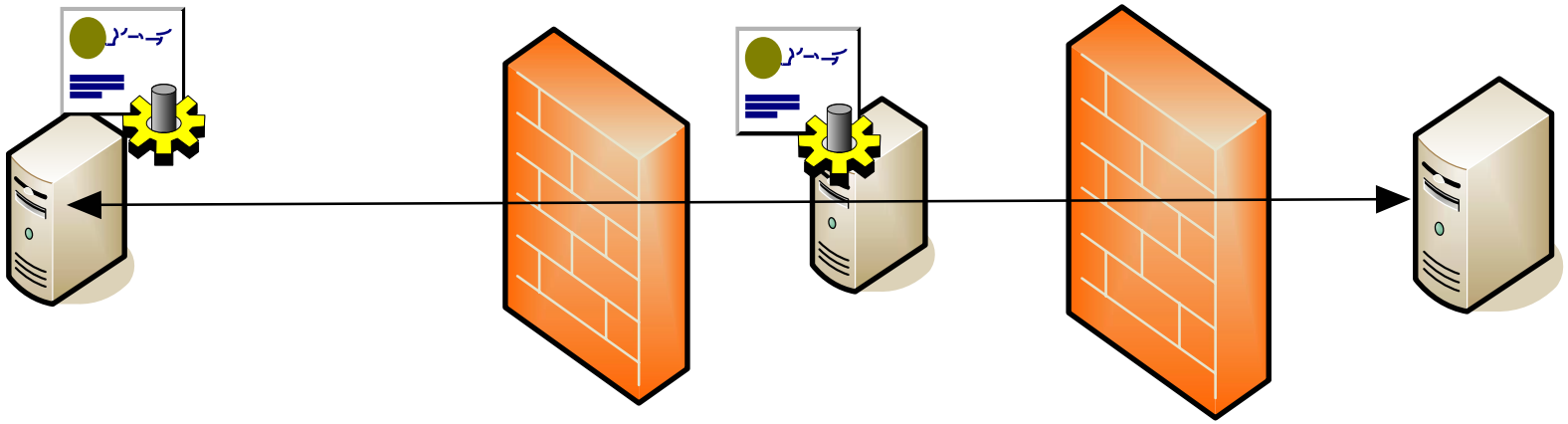
Minimum Authentication Recommendation: C2B/Internal User



Note: If you also have external users, use same (DMZ) proxy and 2 factor authentication for all users

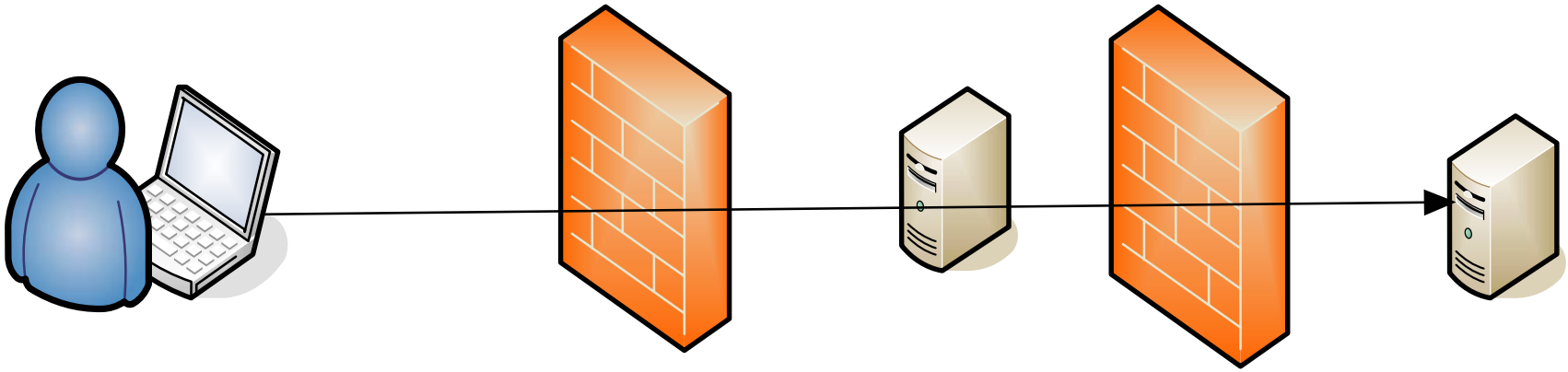
Minimum Authentication Recommendation: B2B Applications

B2B: SSL with Client-Certificate based Authentication



Minimum Authentication Recommendation: C2B/External User

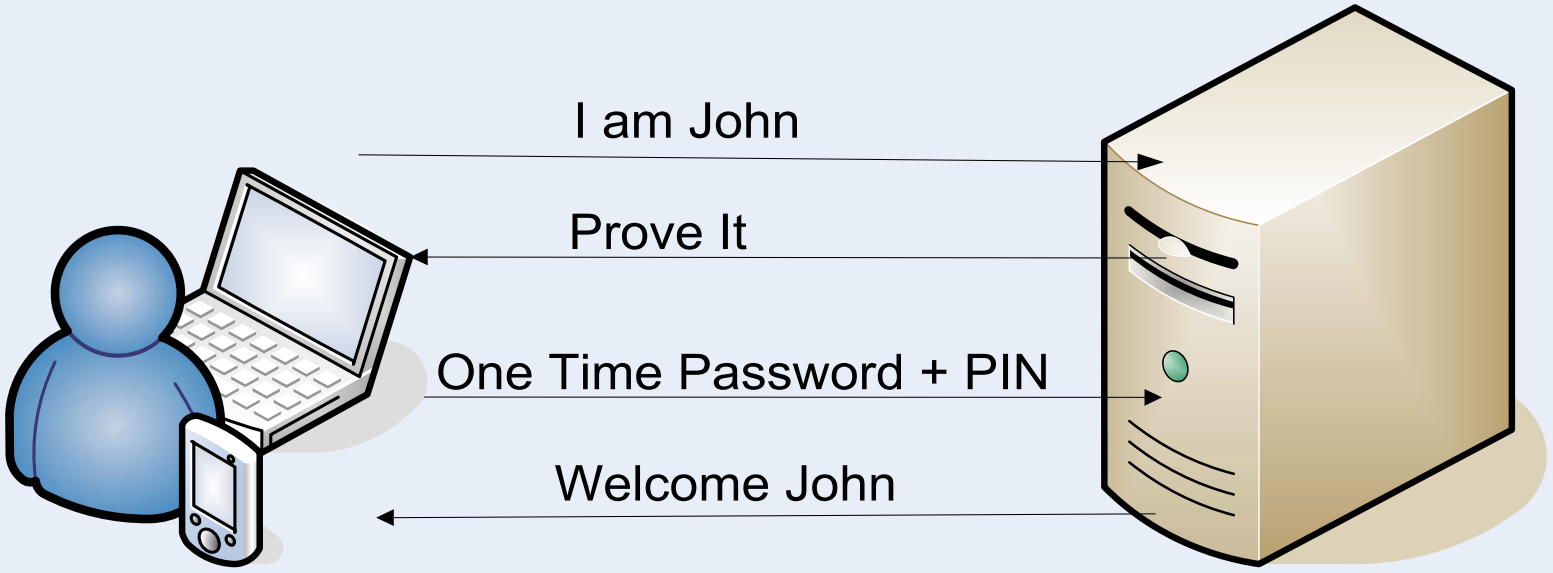
External User: Two Factor Authentication



What is Two Factor Authentication and Why do we need it?

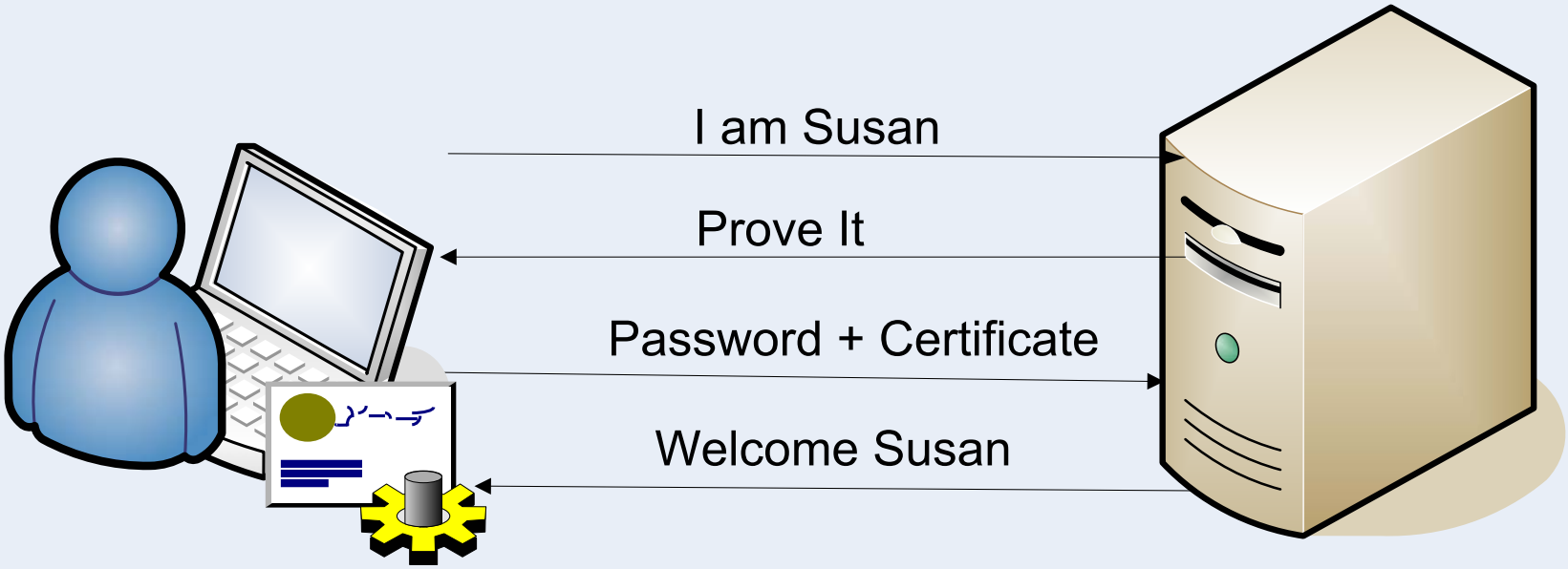
- Authentication Factors
  - What I know (password, PIN)
  - What I have (token, private key)
  - Who I am (thumbprint, retina, voice)
- Two Factor Authentication
  - What I know + what I have (PIN + token)
  - What I know + who I am (PIN + thumbprint)
- Strong Identity Assurance – harder to spoof

Two Factor Authentication – One Time Password (Secure Token)



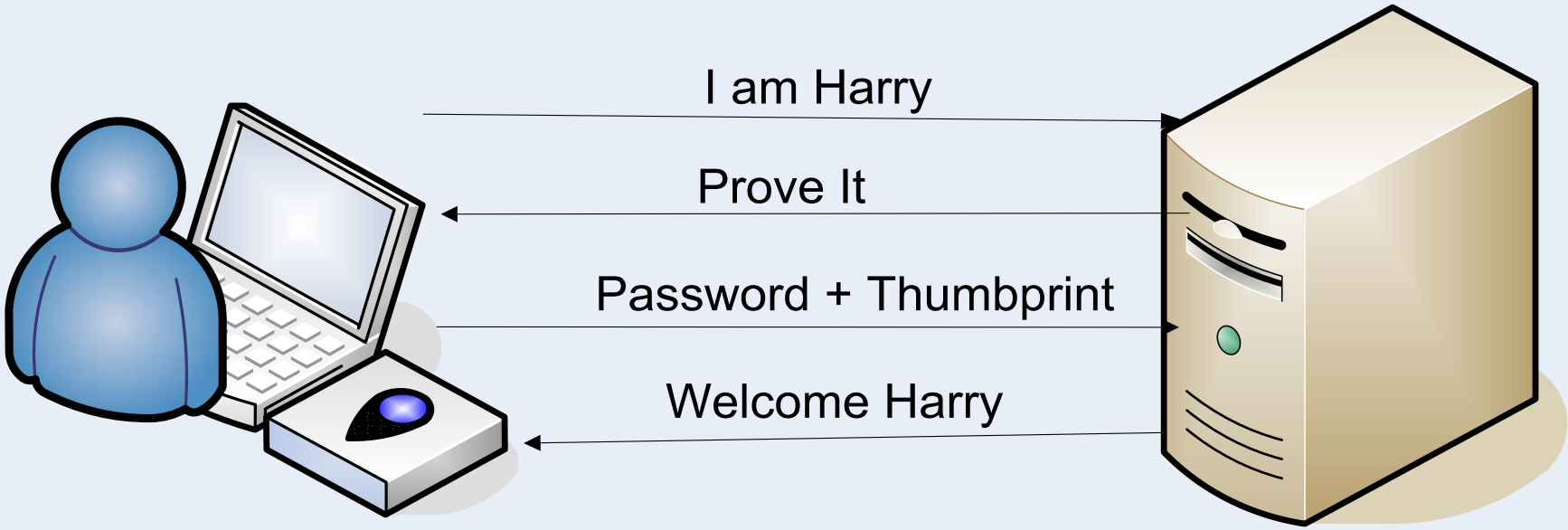
Secure Token based 2-factor Authentication

Two Factor Authentication - Digital Certificates



Certificate based 2-factor Authentication

Two Factor Authentication - Biometrics



Biometric Authentication

Authentication Mechanisms – System Differentiation

Mobility / Ease of Use

- Digital Certificates
  - PKCS12 Files
  - Suited for laptop users
- One time passwords (Secure Tokens)
  - Key-fob: Mobile
  - Smart Cards: Need card, readers
- Biometrics
  - Hardware/software readers

Authentication Mechanisms – System Differentiation

Assurance Level / Accuracy

- Digital Certificates
  - Binary match
- One time password (Secure Token)
  - Binary match
- Biometrics
  - Fuzzy match
  - False positives/negatives possible

Authentication Mechanisms – System Differentiation

Use in Automated Authentication Handshaking (B2B)

- Digital Certificates
  - Open standards based (X.509, SSL)
  - Digital Signatures (XMLDSIG)
  - Interoperable
- One time passwords (Secure Tokens)
  - Proprietary, domain specific
- Biometrics
  - Proprietary, domain specific

Authentication Mechanisms – System Differentiation

Cost

System	Users	Deployment Cost (approximate)
Digital Certificates	1000	$100,000 - $200,000
Secure Tokens	1000	$60,000 - $100,000
Biometrics	1000	$100,000

- Deployment cost based on market leaders (low cost alternatives exist)
- Lifecycle management costs are implementation and environment dependent.

And the winner is?

Depends on your PHIN usage:

- Digital Certificates - only technology that supports Open Standards based Interoperability for
  - Automated B2B authentication (e.g., PHIN web-services)
  - Asymmetric key based encryption for messaging
  - Digital Signatures for communication non-repudiation
- Secure token (key-fob) - mobility and ease of use for C2B authentication
- Digital certificates needed for server authentication (SSL)

Authentication - Approach A

- Users authenticate to a DMZ web-server (proxy) using password + client certificates over SSL
- B2B applications authenticate to a DMZ proxy web-server using client certificates over SSL
- Suited for relatively static user populations or for laptop users
- Single authentication infrastructure to implement and manage

Authentication – Approach B

- Users authenticate to DMZ web-server (proxy) using key-fob
- External B2B applications authenticate to DMZ using client certificates over SSL
- May be required if user population is highly mobile
- Two infrastructures to manage/keep in sync

Other Perimeter Security Considerations

- Authorization, Access Control, User Identity Lifecycle Management
- Single Sign-on

Questions?

rok9@cdc.gov
kailar@bnetal.com

SAFER • HEALTHIER • PEOPLE™